REMARKS

The Examiner has rejected Claims 8-14 and 23 under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Such rejection is deemed moot in view of the clarifications made hereinabove to such claims.

The Examiner has further rejected Claims 1-23 under 35 U.S.C. 102(b) as being anticipated by Klaus (U.S. Patent No.: 5,892,903). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove.

For example, the Examiner relies on the following excerpt from Klaus to meet applicant's claimed "determining a first set of ports required for communicating with network components subject to the risk-assessment modules associated with the risk-assessment scan," and "executing a port scan of the first set of ports."

> "This inventive system operates by sending sync messages to each port on every computer on the network and building a table of service identifiers which identify those ports which responded with a message indicating the presence of a service." (see col. 7, lines 41-45)
>
> "The process implemented by system 40 of FIG. 4 is shown in FIG. 5. The process begins with communication initiation message generator 42 obtaining a destination address of a computer on network 12 from source/destination address generator 34 (Block 200) and the destination port address is set to the first port address on the destination computer (Block 202). Most computers in a TCP/IP protocol have port addresses in the range of 0-65,535. Preferably, each port address is tested by system 40. A communication initiation message is generated for the first port address of the computer at the destination address and passed to transport layer 22 (Block 206). After the communication initiation message is transmitted, response evaluator 44 waits for receipt of a response message from the port to which the communication initiation message was sent (Block 210). Response evaluator 44 then determines whether the message is a handshake acknowledgment message (Block 212). If it is, response evaluator 44 stores a service indicator, the destination address and port address in service topology table (Block 216). In a TCP/IP network, a sync/ack message indicates a service is coupled to the port while a reset message indicates no service is coupled to the port. The process then checks to see if the port address is the last possible port address on the computer (Block 218). If it is not, the port address is incremented (Block 220) and a new communication initiation message is sent to the next port address

> of the computer at the destination address (Block 206). The process continues until all of the port addresses on a computer have been tested to determine whether a service is coupled to each port. After each port has been checked for a service, the process determines whether another destination address is available (Block 224). If there is, another destination address is obtained (Block 200) and the process continues at the first port address for the next computer. The process terminates when all of the computers on network 12 have been checked." (see col. 11, line 59 - col. 12, line 27)

Applicant respectfully disagrees this assertion. In particular, Klaus discloses that "each port address is tested by [its] system." In sharp contrast, applicant teaches and claims a port scan that is limited to a "first set of ports" where the first set of ports is determined to be those "required for communicating with network components subject to the risk-assessment modules associated with the risk-assessment scan." To this end, Klaus's complete port scan does not meet applicant's limited port scan (as claimed), and further *teaches away from* such a technique by the inclusion of all ports.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Klaus reference, for the reasons noted above. Nevertheless, despite the foregoing paramount difference and in the spirit of expediting the prosecution of the present application, applicant now claims in independent Claims 1, 8, and 15, the following (or substantially similar, but not identical) subject matter:

> executing a port scan of the first set of ports associated with the selected risk-assessment modules, for reducing the number of ports scanned during the port scan, wherein latency is reduced" (emphasis added).

Furthermore, applicant now claims in independent Claims 22 and 23, the following (or substantially similar, but not identical) subject matter:

executing a port scan of the set of ports associated with the selected risk-assessment modules and the network components, for reducing the number of ports scanned during the port scan, wherein latency is reduced (emphasis added).

Thus, now emphasized, even more than before, is applicant's claimed technique of limiting the scope of the port scan, in a further effort to reduce latency, particularly with respect to the port scan. Again, it is emphasized that Klaus *teaches away* from such technique by virtue of its all-inclusive port scan.

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

With respect to the dependent claims, applicant has carefully reviewed the excerpts relied upon by the Examiner to reject the same, and has found serious deficiencies in the Examiner's application of the prior art. Just by way of example, the Examiner relies on the following excerpt from Klaus to meet applicant's claimed "wherein a plurality of the risk-assessment modules each have the same port associated therewith, and redundancy in the first set of ports is removed prior to executing the port scan" (see Claim 2 et al.).

> "This embodiment of the inventive system may be coupled with one or more of the other embodiments which generate service command messages to eliminate ports from the attempts to detect vulnerable services. Such a system speeds the security analysis of a network." (see col. 7, lines 56-60)

After carefully reviewing such excerpt and the remaining Klaus reference, however, it is clear that Klaus does not even suggest a technique for dealing with redundancies, as claimed, namely whereby when a plurality of the risk-assessment modules each have the same port associated therewith, a redundancy in the first set of ports is removed prior to executing the port scan. Again, this unique technique further combats latency by avoiding scanning a port more than once.

Still yet, the Examiner relies on the following excerpt from Klaus to meet applicant's claimed "performing the vulnerability checks of the risk-assessment module if the port associated with the risk-assessment module matches at least one port of the stored third set of ports" (see Claim 6 et al.), and "wherein the risk-assessment module is disabled if the port associated with the risk-assessment module does not match at least one port of the stored third set of ports" (see Claim 7 et al.).

> "In this manner, the inventive system may build a map of those ports of each computer on the network which have service coupled thereto without creating a log of any communication connections on any the computers on the network. Since communication connections are only established and logged when the originating computer sends the ack message, this embodiment generates a map of available services in a stealth manner. This embodiment of the inventive system may be coupled with one or more of the other embodiments which generate service command messages to eliminate ports from the attempts to detect vulnerable services. Such a system speeds the security analysis of a network." (see col. 7, lines 48-60)

Such excerpt from Klaus reference, however, merely discloses the exclusion of ports from vulnerability detection. There is simply no performance of vulnerability checks of the risk-assessment module or disabling thereof, based on whether the port associated with the risk-assessment module matches at least one port of the stored third set of ports, as claimed.

Again, the foregoing anticipation criterion has simply not been met. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the following additional dependent claims that have been added for full consideration:

"wherein a port scan involving all 65,536 ports is avoided" (see Claim 24); and

"wherein the risk-assessment modules include a web server vulnerability module with a predetermined port of 80, an e-mail vulnerability module with a predetermined port of 31337, and a Trojan program vulnerability module with a predetermined port of 25" (see Claim 25).

Yet again, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P009/01.114.01).

Respectfully submitted,

By: _____ Date: 12/22/04

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, PC
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573